AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) An optical disk ~~for storing data comprising a decryption module, said module~~ comprising:

   encrypted data, encrypted using at least one secret key;

   a memory including the at least one secret key;

   a cryptoprocessor configured to decrypt the encrypted data ~~of said disk from said~~ using the at least one secret key to obtain decrypted data; and

   a data exchange means configured to send the encrypted data ~~for applying the data of said disk~~ to the cryptoprocessor and read[[ing]] the decrypted data [[of]] from the cryptoprocessor.

2. (Currently Amended) The optical disk ~~according to~~ of claim 1, ~~characterised in that said decryption module~~ wherein cryptographic processor comprises a chip with an integrated circuit.

3. (Currently Amended) The optical disk ~~according to~~ of claim 1, ~~characterised in that said decryption module~~ wherein the cryptoprocessor is integrated in a central zone of [[said]] the optical disk.

4. (Currently Amended) The optical disk ~~according to~~ of claim 1, ~~characterised in that~~ wherein the data exchange means is integrated in a central zone of the optical disk.

5. (Currently Amended) The optical disk ~~according to~~ of claim 1, ~~characterised in that said~~ wherein the optical disk further comprises a balancing means for balancing [[said]] the optical disk.

6. (Currently Amended) The optical disk ~~according to~~ of claim 1, ~~characterised in that~~ wherein the data exchange means ~~is fitted with~~ comprises contacts.

7. (Currently Amended) The optical disk ~~according to~~ of claim 1, ~~characterised in that~~ wherein the data exchange means is fitted with a means for transmitting an energy field.

8. (Currently Amended) A method for reading an ~~data storage~~ optical disk comprising the following stages:

an application stage wherein encrypted data stored on the optical disk is sent ~~in which data of said disk are applied~~ to a cryptoprocessor via a data exchange means;

a decryption stage wherein ~~in which~~ the cryptoprocessor uses at least one secret key to decrypt[[s]] the encrypted data to obtain decrypted data ~~of said disk from a key~~; and

an extraction stage ~~in which~~ wherein the decrypted data [[of]] is read from the cryptoprocessor ~~are read~~ via [[a]] the data exchange means;

wherein the optical disk comprises a decryption module,

wherein [[said]] the decryption module compris[[ing]]es a memory including the at least one secret key, [[a]] the cryptoprocessor, and [[a]] the data exchange means.

9. (Currently Amended) The method ~~according to~~ of claim 8, further comprising an additional stage according to which:

prior to the decryption stage, the encrypted data is modified into a format ~~able to be~~ understood by the cryptoprocessor ~~by means of~~ using a cryptoprocessor interface, wherein the cryptoprocessor interface is included in an optical disk reader.

10. (Currently Amended) The method ~~according to~~ of claim 8, further comprising an additional stage according to which:

prior to the decryption stage, the encrypted data is modified into a format ~~able to be~~ understood by the cryptoprocessor ~~by means~~ using of a cryptoprocerssor interface, wherein the cryptoprocessor interface is included in a computer.

11. (Currently Amended) The method ~~according to~~ of claim 8, wherein the optical disk further comprises non-encrypted data and wherein ~~characterised in that~~ in the decryption stage the cryptoprocessor decrypts the encrypted data and the non-encrypted data ~~is systematically decrypted, whether said data is encrypted or not~~.

12. (Currently Amended) The method ~~according to~~ of claim 8, further comprising an additional stage according to which:

a set of unprocessed data and a set of decrypted data are loaded ~~into~~ onto a computer

wherein both sets of data originat[[ing]]e from a set of data read [[in]] from the optical disk.

13. (Currently Amended) The method ~~according to~~ of claim 12, ~~characterised in that loading is made alternately~~ wherein the set of unprocessed data and the set of decrypted data are load onto the computer in an alternating manner.

14. (Currently Amended) The method ~~according to~~ of claim 12, ~~characterised~~ wherein ~~in that a~~ the set of unprocessed data comprises ~~a zone of~~ unusable encrypted data[[,]] and [[a]] the set of decrypted data comprises ~~a zone of~~ usable decrypted data.

15. (Currently Amended) The method ~~according to~~ of claim [[12]] 14, ~~characterised in that a~~ wherein the set of unprocessed data comprises ~~a zone of~~ usable-non-encrypted data[[,]] and [[a]] the set of decrypted data comprises ~~a zone of~~ unusable decrypted data.

16. (Currently Amended) The method ~~according to~~ of claim [[14]] 15, further comprising an additional stage according to which:

an executable code portion in ~~a useful data zone including application data~~ one selected from a group consisting of usable-non-encrypted data and usable decrypted data is executed.

17. (Currently Amended) The method ~~according to~~ of claim 16, further comprising an additional stage according to which:

~~various data zones are interconnected,~~ new data is loaded into the memory and a data zone is reconstituted with the aid of a set of links included in the executable code.

18. (Currently Amended) A disk reader device configured to ~~placed to~~ read an optical ~~data storage~~ disk, comprising:

~~said device including~~

an interface for exchanging data with a decryption module,

wherein the decryption module is located on the optical disk,

wherein the decryption module comprises:

a memory including at least one secret key,

a cryptoprocessor configured to decrypt [[the]] encrypted data stored on the optical disk using the at least one secret key ~~of said disk from said key~~, and

a data exchange means [[for]] configured to receive encrypted data from the interface, send the encrypted data ~~applying the data of said disk~~ to the cryptoprocessor, [[and]] read[[ing]] the decrypted data ~~of the~~ from the cryptoprocessor, and send the decrypted data to the interface.

19. (Currently Amended) A method for protecting an optical ~~data storage~~ disk comprising:

an encryption stage ~~in which~~ wherein data is encrypted to obtain encrypted data using ~~from~~ at least one [[sole]] secret key ~~so as to obtain encrypted data~~;

a writing stage ~~in which~~ wherein the encrypted data [[are]] is written ~~in said~~ to an optical disk; and

a loading stage ~~in which~~ wherein the at least one secret key is loaded into a memory of a decryption module[[;]],

wherein said optical ~~data storage~~ disk comprises [[a]] the decryption module that includes ~~comprising a~~ the memory, a cryptoprocessor, and a data exchange means,

wherein the cryptoprocessor is configured to decrypt the encrypted data.

20. (Currently Amended) A method for protecting an optical disk ~~for storing data~~, comprising:

decrypting encrypted data stored on the optical disk by a portable object using ~~of said disk with the aid of~~ a secret key,

wherein the secret key is stored ~~included~~ in a memory,

wherein the memory is located in [[of a]] the portable object,

wherein the portable object is integrated in [[said]] the optical disk, and

wherein the secret key is not communicated outside of the portable object ~~remaining inside said object~~ during decryption of the encrypted data, and

exchanging the encrypted data ~~of said disk~~ between [[said]] the portable object and [[said]] the optical disk ~~by means of~~ using a data exchange means integrated in [[said]] the optical disk.

21. (Currently Amended) The method ~~according to~~ of claim 20, ~~characterised in that said~~ wherein the portable object comprises a chip with an integrated circuit.

22. (Currently Amended) The method ~~according to~~ of claim 20, ~~characterised in that~~ wherein the decryption stage is carried out using a cryptoprocessor integrated in [[said]] portable object.

23. (Currently Amended) The method ~~according to~~ of claim 22, further comprising ~~an additional stage according to which~~:

prior to ~~the decryption stage~~ decrypting the encrypted data, [[the]] modifying the encrypted data ~~is modified~~ into a format ~~able to be~~ understood by the cryptoprocessor via a cryptoprocessor interface included in an optical disk reader.

24. (Currently Amended) The method ~~according to~~ of claim 22, further comprising ~~an additional stage according to which~~:

prior to the ~~decryption stage~~ decrypting the encrypted data, the encrypted data is modified into a format ~~able to be~~ understood by the cryptoprocessor ~~by means of~~ using a cryptoprocessor interface included in a computer.

25. (Currently Amended) The method ~~according to~~ of claim 20, ~~characterised in that~~ wherein the optical disk further comprises non-encrypted data and wherein the cryptoprocessor decrypts the encrypted data and the non-encrypted ~~the data is decrypted systematically regardless of whether said data was originally encrypted or not~~.

26. (Currently Amended) The method ~~according to~~ of claim 20, further comprising ~~an additional stage according to which~~:

loading a set of unprocessed data and a set of decrypted data ~~are loaded~~ into a computer wherein both sets of data originat[[ing]]e from a set of data read in the optical disk.

27. (Currently Amended) The method ~~according to~~ of claim 26, ~~characterised in that loading is made alternately~~ wherein the set of unprocessed data and the set of decrypted data are load onto the optical disk in an alternating manner.

28. (Currently Amended) The method ~~according to~~ of claim 26, ~~characterised~~ wherein ~~in that a~~ the set of unprocessed data comprises ~~a zone of~~ unusable encrypted data, and [[a]] the set of decrypted data comprises ~~a zone of~~ usable decrypted data.

29. (Currently Amended) The method ~~according to~~ of claim [[26]] 28, ~~characterised in that a~~ wherein the set of unprocessed data comprises ~~a zone of~~ usable-non-encrypted data[[,]] and [[a]] the set of decrypted data comprises ~~a zone of~~ unusable decrypted data.

30. (Currently Amended) The method ~~according to~~ of claim [[28]] 29, further comprising ~~an additional stage according to which~~:

executing one executable code portion included in one selected from a group consisting of usable-non-encrypted data and usable decrypted data ~~the useful data zone is executed including application data~~.

31. (Currently Amended) The method ~~according to~~ of claim 30, further comprising ~~an additional stage according to which~~:

~~at least two data zones are interconnected,~~

loading new data ~~is loaded~~ into the memory, and

reconstructing a data zone ~~is reconstructed with the aid of~~ using a set of links included in the executable code.

32. (Currently Amended) The method ~~according to~~ of claim 20, further comprising ~~an additional stage according to which~~:

encrypting data ~~is encrypted by means of~~ using [[a]] the secret key;

storing the encrypted data on the optical disk

~~, wherein said encrypted data is written in said disk~~.

33. (Currently Amended) The method ~~according to~~ of claim 20, wherein [[said]] optical disk [[data]] ~~forms~~ comprises at least one application written in a high-level language.

34. (Currently Amended) The method ~~according to~~ of claim 33, wherein the encrypted data comprises at least a portion of the application ~~characterised in that the application is at least partially encrypted~~.

35. (Currently Amended) The method ~~according to~~ of claim 15, wherein the method comprises an additional stage comprising executing an executable code portion in one selected from a group consisting of usable-non-encrypted data and usable decrypted data ~~a useful data zone including application data~~.

36. (Cancelled)

37. (Currently Amended) The method ~~according to~~ of claim 29, wherein the method comprises an additional stage comprising executing one executable code portion included in one selected from a group consisting of usable-non-encrypted data and usable decrypted data ~~the useful data zone, said code portion including application data~~.